A Procedure for Analyzing the Software and Operational Impact of Software/Hardware Interface Anomalies

Robert E. Loesh
Willie J. Fitzpatrick, Jr.
Richard M. Wyskida

April 2, 2003

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE **02 APR 2003**	2. REPORT TYPE	3. DATES COVERED **00-00-2003 to 00-00-2003**

4. TITLE AND SUBTITLE
A Procedure for Analyzing the Software and Operational Impact of Software/Hardware Interface Anomalies

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
U.S. Army Research, Development and Engineering Command,Software Engineering Directorate,Redstone Arsenal,AL,35898

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES
2004 Southeastern Software Engineering Conference, Huntsville, AL, 29-31 March 2004

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**Same as Report (SAR)**	**28**	

Introduction

- Software Failure Modes, Effects, and Criticality Analysis Special Assessment Procedure (FMASAP:1-1) is one of the 16 Procedures that make up the SED Software Engineering Evaluation System (SEES).

Note: For information concerning the other 15 SEES procedures, contact:
jackie.langhout@sed.redstone.army.mil
256-876-3038

Introduction (Cont’d)

- FMASAP is applicable to Systems which possess one or more of the following characteristics:
  - Fault Tolerant
  - Safety-Critical
  - Embedded
  - Real-time

Introduction (Cont'd)

- Purpose of FMASAP is to determine:
  - Potential system failures and criticality.
  - Root causes for critical hardware and interface failures.
  - Software resilience to hardware interface anomalies.
  - Operational impacts of software responses to hardware failures.

Note: FMASAP is not intended to address software-to-software interfaces, but could be tailored to address them in concert with Fault Tree Analysis.

Introduction (Cont'd)

- FMASAP is recommended to be performed at PDR, CDR, and completion of CUT.
- When System Modes exist, perform the FMASAP procedures as a separate set of analyses (i.e., each System mode requires a unique set of RRLF and SFMECAF forms).

Note: It is recommended the FMASAP be performed on a continuing basis to ensure accurate results at the end of the development and to address approved Engineering Change Proposals.

Introduction (Cont’d)

- FMA identifies Single Point interface failures only. To address Multiple Point interface failures, extend the Single Point FMA analysis by identifying the multiple interfaces.

Introduction (Cont'd)

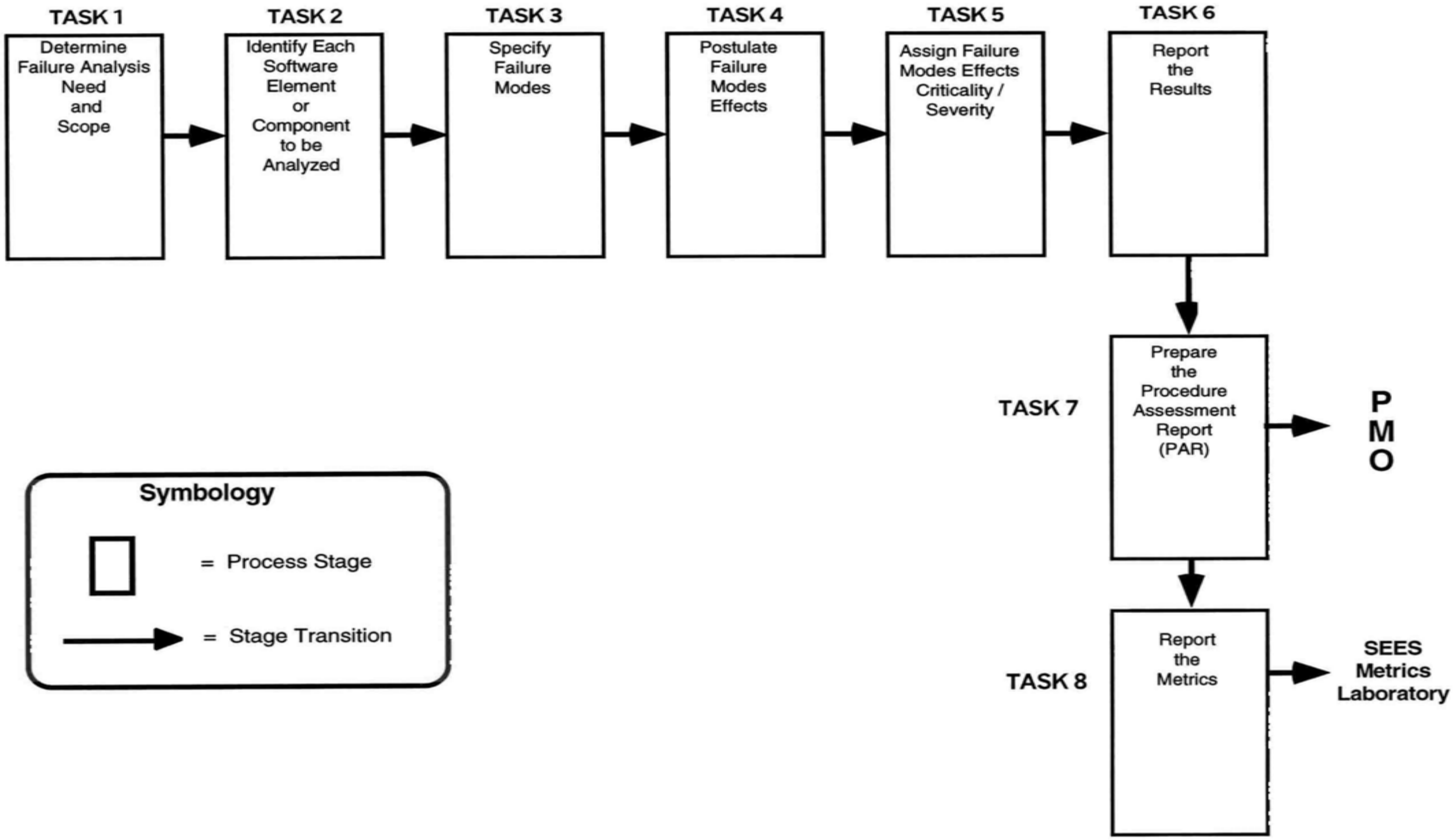

TASK 1
Determine Failure Analysis Need and Scope
TASK 2
Identify Each Software Element or Component to be Analyzed
TASK 3
Specify Failure Modes
TASK 4
Postulate Failure Modes Effects
TASK 5
Assign Failure Modes Effects Criticality / Severity
TASK 6
Report the Results
TASK 7
Prepare the Procedure Assessment Report (PAR)
PMO
TASK 8
Report the Metrics
SEES Metrics Laboratory
Symbology
= Process Stage
= Stage Transition

Figure 1-1 Software Failure Modes, Effects, and Criticality Analysis SAP Flow Chart

TASK 1
Determine Failure Analysis Need and Scope

- Purpose: Scope (Delimit) the analysis:
  - Specify System Reliability, Fault Tolerant, and Safety requirements and policies.
  - Specify associated hardware interfaces.
  - Identify associated software to be analyzed.

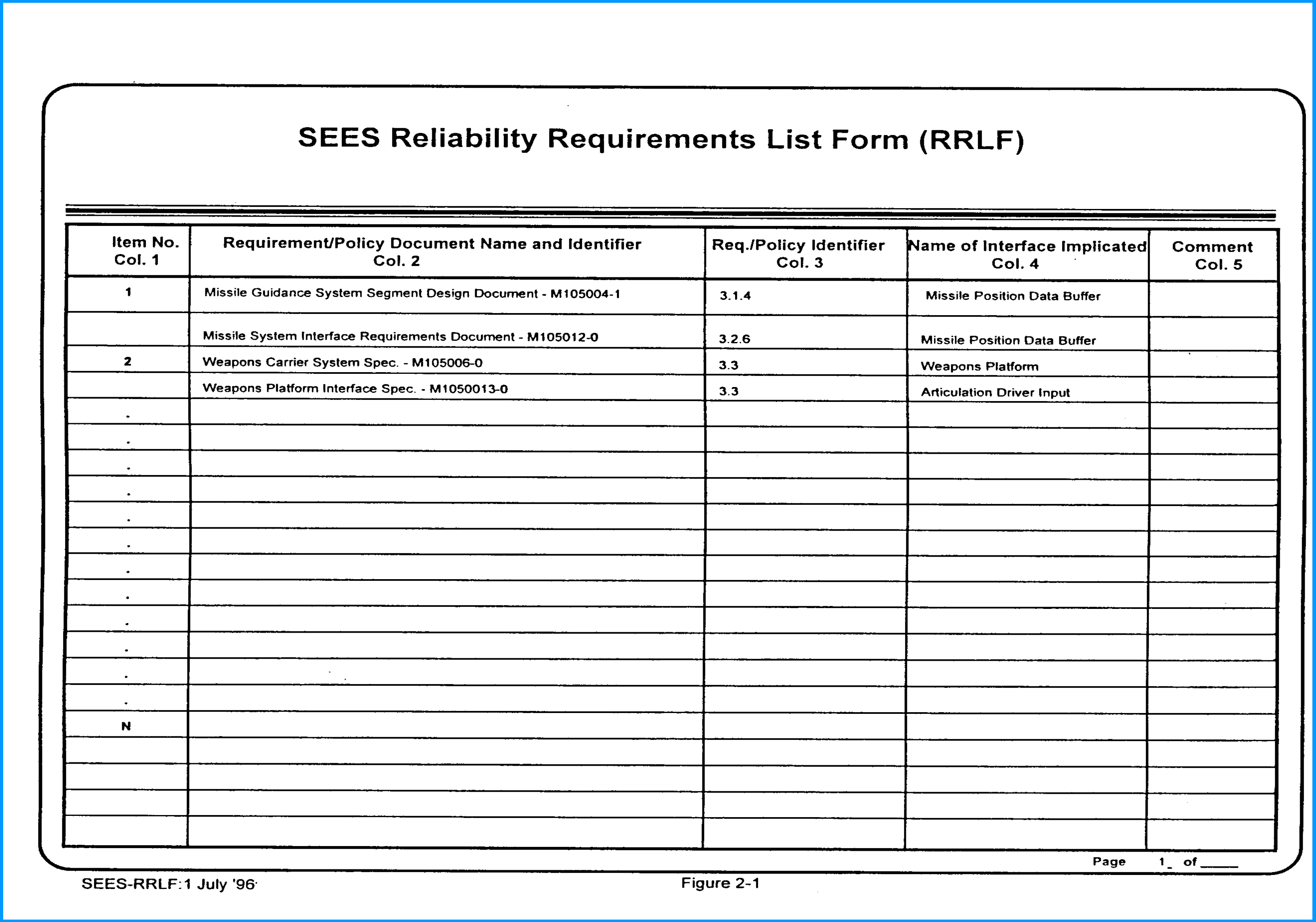
TASK 1
Determine Failure Analysis Need and Scope (Cont'd)

- Determine resilience of software design to accommodate discrete hardware interface anomalies including:
  - Continuous input signals due to electrical shorts.
  - Single event upsets.
  - Intermittent operations.
  - Input Buffer overflow.
  - Lost interrupts/control signals.
  - Defective Direct Memory Access operations.
  - Defective clocks and timers.
  - Transmission Errors/Device Inoperability.

TASK 1
Determine Failure Analysis Need and Scope (Cont'd)

Step 1: Determine the System/Software Reliability, Fault Tolerant, & Safety Requirements/Policy (Col. 1, 2, & 3)

- Data information sources include:
  - System Specification.
  - Project/Program Policies & SOW.
  - System Interface Control Documents.
  - Interface Requirements Specifications (IRSs).
  - System/Segment Design Document (SSDD).
  - Subsystem Design Documents.



SEES Reliability Requirements List Form (RRLF)

Item No. Col. 1	Requirement/Policy Document Name and Identifier Col. 2	Req./Policy Identifier Col. 3	Name of Interface Implicated Col. 4	Comment Col. 5
1	Missile Guidance System Segment Design Document - M105004-1	3.1.4	Missile Position Data Buffer	
	Missile System Interface Requirements Document - M105012-0	3.2.6	Missile Position Data Buffer	
2	Weapons Carrier System Spec. - M105006-0	3.3	Weapons Platform	
	Weapons Platform Interface Spec. - M1050013-0	3.3	Articulation Driver Input	
.				
.				
.				
.				
.				
.				
.				
.				
.				
.				
.				
.				
N				

Page 1_ of ____

SEES-RRLF:1 July '96

Figure 2-1

TASK 1
Determine Failure Analysis Need and Scope (Cont'd)

Step 2: Specify the hardware interface involved (Col. 4).

Step 3: Identify associated software subsystem/CSCI (Col.5).

Note: Task 1 can be skipped if specific or all hardware/software interfaces are to be analyzed.

TASKs 2 – 5
Complete SFMECAF

- RRLF entries scope areas needing analysis.
- The Software Failure Modes, Effects and Criticality Analysis Form (SFMECAF) documents the analysis.
- The SFMECAF has an entry for each RRLF entry that has software associated with it.
- SFMECAF Column 1 correlates directly to the RRLF Column 1.

SEES Software Failure Modes, Effects, and Criticality Analysis Form (SFMECAF)

Program ID Sure Shot Missile

Technical Lead J. Amcom

Analysis Date: 3/1/96

System: Missile Guidance

RRLF Item No. Col. 1	Interface Data Col. 2	System Hardware Interface Col. 3	Software Element Col. 4	System Failure Modes Col. 5	Effects Col. 6	Criticality Col. 7	Comments/Rec. Sw/Hw Changes Col. 8
1	a. Position	a. Radar Input	a. Missile CSCI	1. No Data	1. No Nav. command updates	1. Catastropic	1. Use backup system
	Coordinates	Buffer		2. Data	2. Erratic cmds. generated and	2. Critical	inputs after checking if
	b. Time	b. Radar Input	b. Missile CSCI	Inconsistant	operator error message		missile position data is
		Buffer		with Missile			reasonable and available.
				Status			2. (Same as 1 above.)
				3. Irregular data	3. Erratic Nav. cmds. and	3. Critical	3. Implement dead
				values (out of			reckon algorithm and/
				reasonableness			or use backup system
				range)			missile position data.
				4. Input timing	4. Missile guidance precision	4. Marginal	4. (Same as 3 above.)
				incorrect	loss		
2	a. Angle and	a. Platform Input	a. Platform	1. No Data	1. No positioning and Weapon	1. Critical	1. Run Diagnostics
	Azimuth Data	Registers	Articulation CSCI		not fired		Reset System
				2. Data inconsistant	2. Weapon not fired	2. Critical	2. Restart System
				with Platform status			
				3. Unreasonable	3. Incorrect Platform/Weapon	3. Catastrophic	3. Verify data for
.				Data	aiming		reasonableness
.							
N							

Page ___ of ___

Figure 3-1

Multiple Point Interface Failures

- FMA identifies Single Point interface failures only. To address Multiple Point interface failures, extend the Single Point FMA analysis by identifying the multiple interfaces in SFMECAF columns 1 through 4 and treating each multiple interface as a single entry by completing the analysis in columns 5 through 8.

TASK 2
Identify Each Software Element to be Analyzed

- Minimize analysis effort by:
  - Focusing on a small subset of software elements involved in the actual processing and affecting the correctness of the hardware interfaces input data.

TASK 2
Identify Each Software Element to be Analyzed (Cont’d)

Step 1: Identify System Input Data and Hardware Devices

a. Enter on the SFMECAF the RRLF Item No. (from Col. 1) being analyzed.

b. For each entry specify the type of interface data (Col. 2) and discrete hardware interface (Col. 3).

Step 2: Specify the Software Elements that process the Discrete Hardware Interface Data (Col. 4).

SEES Software Failure Modes, Effects, and Criticality Analysis Form (SFMECAF)

Program ID Sure Shot Missile

Technical Lead J. Amcom

Analysis Date: 3/1/96

System: Missile Guidance

RRLF Item No. Col. 1	Interface Data Col. 2	System Hardware Interface Col. 3	Software Element Col. 4	System Failure Modes Col. 5	Effects Col. 6	Criticality Col. 7	Comments/Rec. Sw/Hw Changes Col. 8
1	a. Position	a. Radar Input	a. Missile CSCI	1. No Data	1. No Nav. command updates	1. Catastropic	1. Use backup system
	Coordinates	Buffer		2. Data	2. Erratic cmds. generated and	2. Critical	inputs after checking if
	b. Time	b. Radar Input	b. Missile CSCI	Inconsistant	operator error message		missile position data is
		Buffer		with Missile			reasonable and available.
				Status			2. (Same as 1 above.)
				3. Irregular data	3. Erratic Nav. cmds. and	3. Critical	3. Implement dead
				values (out of			reckon algorithm and/
				reasonableness			or use backup system
				range)			missile position data.
				4. Input timing	4. Missile guidance precision	4. Marginal	4. (Same as 3 above.)
				incorrect	loss		
2	a. Angle and	a. Platform Input	a. Platform	1. No Data	1. No positioning and Weapon	1. Critical	1. Run Diagnostics
	Azimuth Data	Registers	Articulation CSCI		not fired		Reset System
				2. Data inconsistant	2. Weapon not fired	2. Critical	2. Restart System
				with Platform status			
				3. Unreasonable	3. Incorrect Platform/Weapon	3. Catastrophic	3. Verify data for
.				Data	aiming		reasonableness
.							
N							

Page ____ of ____

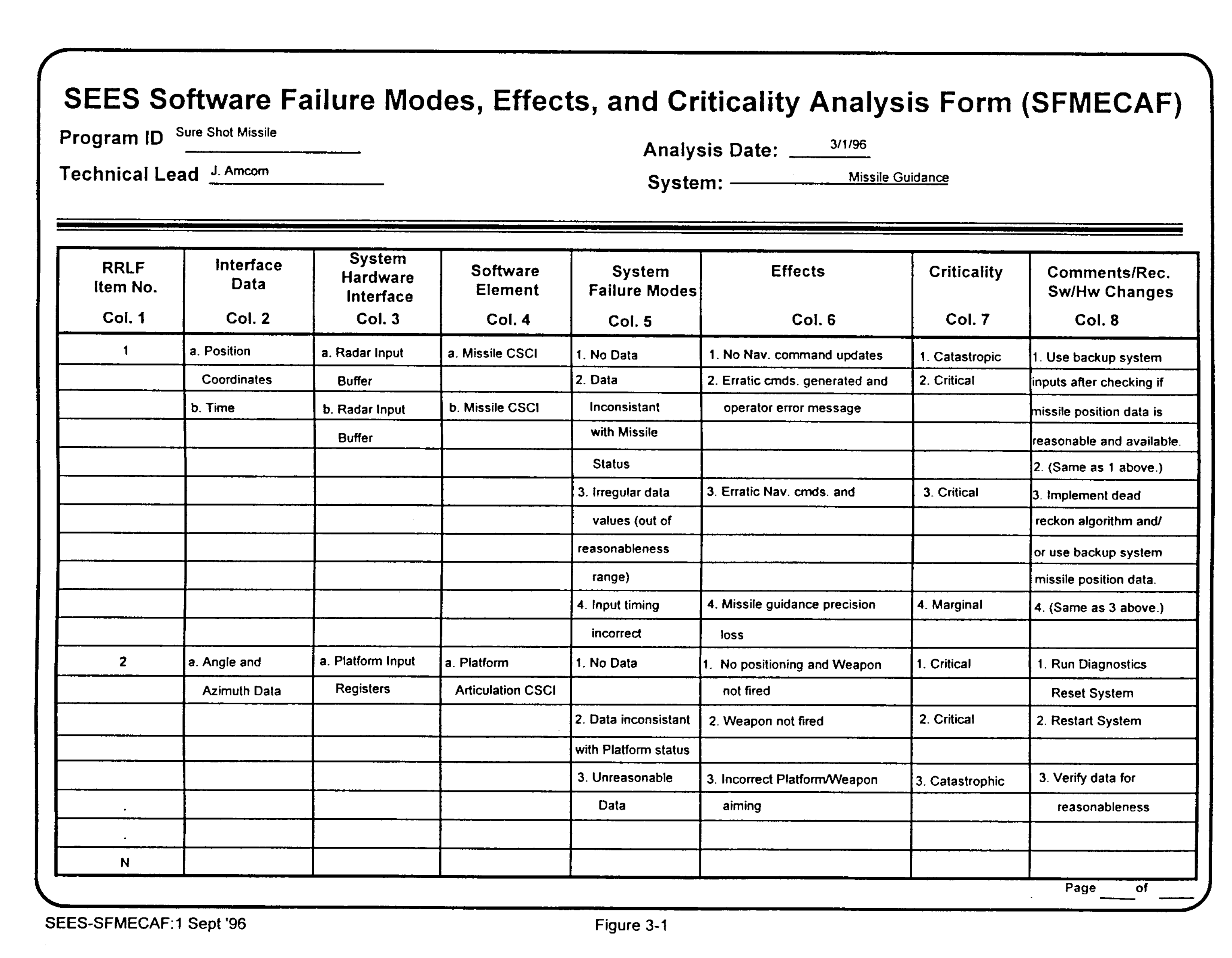
Figure 3-1

TASK 3
Specify Failure Modes

- Identify each possible result of the hardware interface failure (Col. 5), for example:
  - Intermittent Data.
  - Buffer overflow.
  - Lost or overwritten corrupted input data.
  - No Data.
  - Defective time.
  - Incorrect error detection (CRCs, checksums).
  - Inconsistent Data.

TASK 3
Specify Failure Modes (Cont’d)

- Column 5 data is based upon Column 2, 3, and 4, but may have more or less items.
- Permits the determination of:
  - Criticality.
  - Possible corrective action.
  - Testing approaches.



SEES Software Failure Modes, Effects, and Criticality Analysis Form (SFMECAF)

Program ID Sure Shot Missile

Technical Lead J. Amcom

Analysis Date: 3/1/96

System: Missile Guidance

RRLF Item No. Col. 1	Interface Data Col. 2	System Hardware Interface Col. 3	Software Element Col. 4	System Failure Modes Col. 5	Effects Col. 6	Criticality Col. 7	Comments/Rec. Sw/Hw Changes Col. 8
1	a. Position	a. Radar Input	a. Missile CSCI	1. No Data	1. No Nav. command updates	1. Catastropic	1. Use backup system
	Coordinates	Buffer		2. Data	2. Erratic cmds. generated and	2. Critical	inputs after checking if
	b. Time	b. Radar Input	b. Missile CSCI	Inconsistant	operator error message		missile position data is
		Buffer		with Missile			reasonable and available.
				Status			2. (Same as 1 above.)
				3. Irregular data	3. Erratic Nav. cmds. and	3. Critical	3. Implement dead
				values (out of			reckon algorithm and/
				reasonableness			or use backup system
				range)			missile position data.
				4. Input timing	4. Missile guidance precision	4. Marginal	4. (Same as 3 above.)
				incorrect	loss		
2	a. Angle and	a. Platform Input	a. Platform	1. No Data	1. No positioning and Weapon	1. Critical	1. Run Diagnostics
	Azimuth Data	Registers	Articulation CSCI		not fired		Reset System
				2. Data inconsistant	2. Weapon not fired	2. Critical	2. Restart System
				with Platform status			
				3. Unreasonable	3. Incorrect Platform/Weapon	3. Catastrophic	3. Verify data for
.				Data	aiming		reasonableness
.							
N							

Page ____ of ____

SEES-SFMECAF:1 Sept '96

Figure 3-1

TASK 4
Postulate Failure Modes Effects

- Review design at lowest level available.
  - Preliminary Design.
  - Critical Design.
  - Source Code.
- Specify effect on software when failure mode being analyzed occurs (Col. 6).
- For each Column 5 item, there should be a Column 6 item.

SEES Software Failure Modes, Effects, and Criticality Analysis Form (SFMECAF)

Program ID Sure Shot Missile

Technical Lead J. Amcom

Analysis Date: 3/1/96

System: Missile Guidance

RRLF Item No. Col. 1	Interface Data Col. 2	System Hardware Interface Col. 3	Software Element Col. 4	System Failure Modes Col. 5	Effects Col. 6	Criticality Col. 7	Comments/Rec. Sw/Hw Changes Col. 8
1	a. Position	a. Radar Input	a. Missile CSCI	1. No Data	1. No Nav. command updates	1. Catastropic	1. Use backup system
	Coordinates	Buffer		2. Data	2. Erratic cmds. generated and	2. Critical	inputs after checking if
	b. Time	b. Radar Input	b. Missile CSCI	Inconsistant	operator error message		missile position data is
		Buffer		with Missile			reasonable and available.
				Status			2. (Same as 1 above.)
				3. Irregular data	3. Erratic Nav. cmds. and	3. Critical	3. Implement dead
				values (out of			reckon algorithm and/
				reasonableness			or use backup system
				range)			missile position data.
				4. Input timing	4. Missile guidance precision	4. Marginal	4. (Same as 3 above.)
				incorrect	loss		
2	a. Angle and	a. Platform Input	a. Platform	1. No Data	1. No positioning and Weapon	1. Critical	1. Run Diagnostics
	Azimuth Data	Registers	Articulation CSCI		not fired		Reset System
				2. Data inconsistant	2. Weapon not fired	2. Critical	2. Restart System
				with Platform status			
				3. Unreasonable	3. Incorrect Platform/Weapon	3. Catastrophic	3. Verify data for
.				Data	aiming		reasonableness
.							
N							

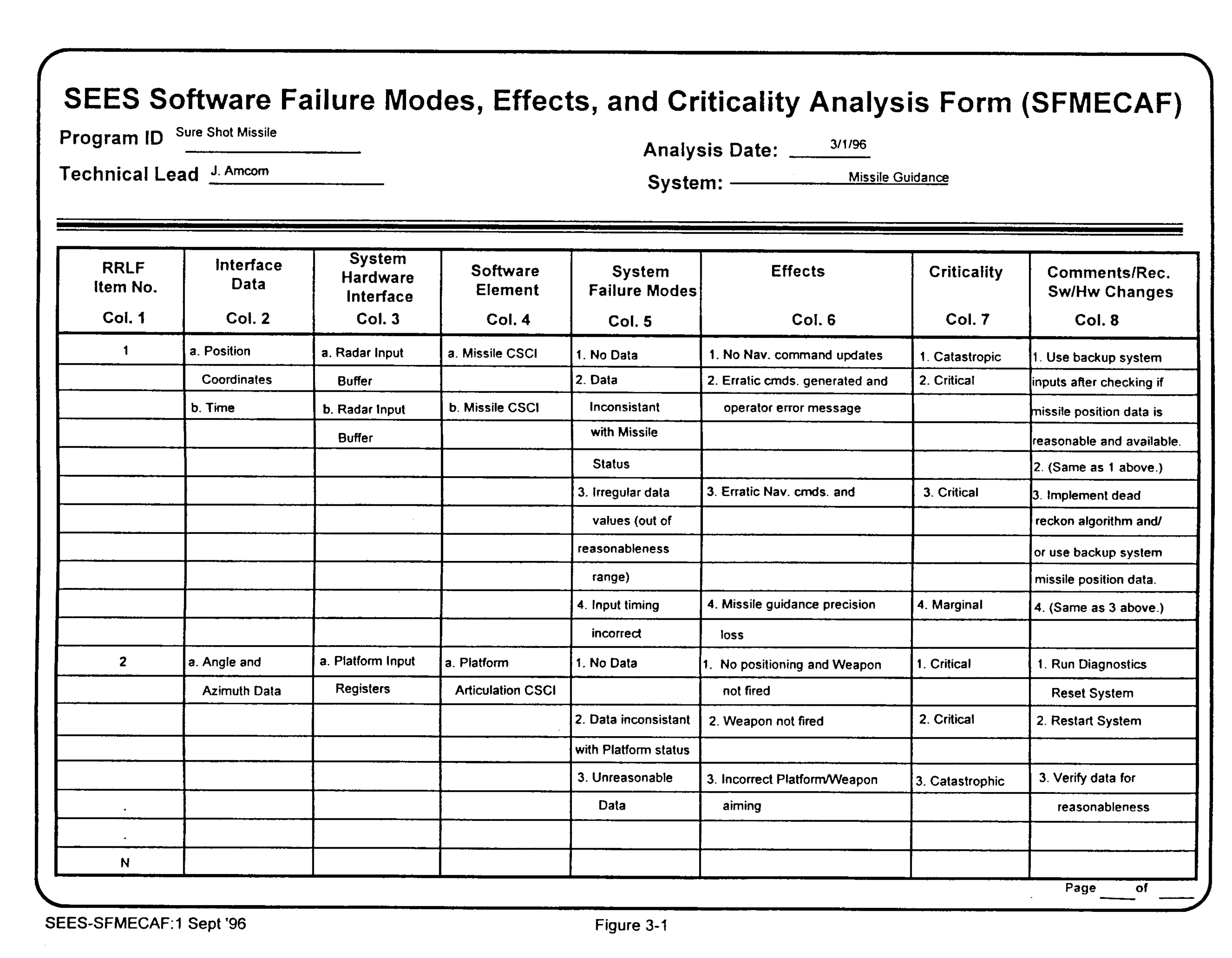
Page ____ of ____

SEES-SFMECAF:1 Sept '96

Figure 3-1

TASK 5
Assign Failure Modes Effects Criticality/Severity

- Specify in Column 7 the criticality/severity of each failure effect item in Column 6. For software design that accommodates the anomaly, the state specified in Column 7 is (NONE).
- There should be an item in Column 7 for each item in Column 6.
- States of Criticality: Severity Classifications per 1629A, 4.4.3, i.e., Category I, II, III, IV, and None.
- Column 8 is optional.



SEES Software Failure Modes, Effects, and Criticality Analysis Form (SFMECAF)

Program ID Sure Shot Missile

Technical Lead J. Amcom

Analysis Date: 3/1/96

System: Missile Guidance

RRLF Item No. Col. 1	Interface Data Col. 2	System Hardware Interface Col. 3	Software Element Col. 4	System Failure Modes Col. 5	Effects Col. 6	Criticality Col. 7	Comments/Rec. Sw/Hw Changes Col. 8
1	a. Position	a. Radar Input	a. Missile CSCI	1. No Data	1. No Nav. command updates	1. Catastropic	1. Use backup system
	Coordinates	Buffer		2. Data	2. Erratic cmds. generated and	2. Critical	inputs after checking if
	b. Time	b. Radar Input	b. Missile CSCI	Inconsistant	operator error message		missile position data is
		Buffer		with Missile			reasonable and available.
				Status			2. (Same as 1 above.)
				3. Irregular data	3. Erratic Nav. cmds. and	3. Critical	3. Implement dead
				values (out of			reckon algorithm and/
				reasonableness			or use backup system
				range)			missile position data.
				4. Input timing	4. Missile guidance precision	4. Marginal	4. (Same as 3 above.)
				incorrect	loss		
2	a. Angle and	a. Platform Input	a. Platform	1. No Data	1. No positioning and Weapon	1. Critical	1. Run Diagnostics
	Azimuth Data	Registers	Articulation CSCI		not fired		Reset System
				2. Data inconsistant	2. Weapon not fired	2. Critical	2. Restart System
				with Platform status			
				3. Unreasonable	3. Incorrect Platform/Weapon	3. Catastrophic	3. Verify data for
.				Data	aiming		reasonableness
.							
N							

Page ____ of ____

SEES-SFMECAF:1 Sept '96

Figure 3-1

Metrics

Failure Mode Deficiencies by Criticality for each Software Design Element

Software Design Element (CSCI, CSU, etc.)	Criticality/Severity			
	I	II	III	IV

Effort Planning Data

Assumption: A CSCI has 100-150 requirements in SRS
and has 3 to 6 hardware interfaces.

		Per CSCI
Task 1	Determine Failure Analysis Need and Scope	5-10 Days
Task 2	Identify Each Software Element or Component to be Analyzed	3-10 Days
Task 3	Specify Failure Modes	2-5 Days
Task 4	Postulate Failure Modes Effects	5-10 Days
Task 5	Assign Failure Modes Effects Criticality/Severity	2-5 Days

Software Failure Modes, Effects, and Criticality Analysis Form (SFMECAF)

RRLF Item No.	Interface Data	System Hdwe. Interface	Software Element	System Failure Modes	Effects/ Detection Method	Criti-cality	Rec. SW/HW Changes	Mitigating Design Feature/ Alternate Operating Procedure	Mitigating Design Feature Failure Detection	Mitigating Tests/ Inspections
Col. 1	Col. 2	Col. 3	Col. 4	Col.5	Col. 6	Col. 7	Col. 8	Col. 9	Col. 10	Col. 11
10B	Stormscope	Emergency Control Plan (ECP)	N/A	No Data - Defective Wire	Loss of Stormscope Data, Present Pos, Relative Bearing to Waypoint, Mag Heading, Next 10 Active Flight Plan Waypoints	4	None	Stormscope Data continues to be available on both CDUs & visuals	None	ATP 21.388 Section 21.0
			CDU CSCI	No Data from CDU	Loss of Stormscope Data, Present Pos, Relative Bearing to Waypoint, Mag Heading, Next 10 Active Flight Plan Waypoints	4	None	Stormscope Data continues to be available on both CDUs & visuals	None	ATP 21.388 Section 21.0
10C	Stormscope	CDU-1553	CDU CSCI	No Data	Loss of Stormscope Data, Present Pos, Relative Bearing to Waypoint, Mag Heading, Next 10 Active Flight Plan Waypoints	4	None	Stormscope Data continues to be available on one or both CDUs & visuals	None	ATP 21.388 Section 12.0
			CDU CSCI	Data Inconsistent with System Status	Pilot Cross Check Stormscope Data Incorrect on Both CDU's	4	None	Stormscope Data continues to be available on one or both CDUs & visuals	None	ATP 21.388 Section 12.0
			CDU CSCI	Data out of Range	Loss of Stormscope Data, Present Pos, Relative Bearing to Waypoint, Mag Heading, Next 10 Active Flight Plan Waypoints	4	None	Stormscope Data continues to be available on one or both CDUs & visuals	None	ATP 21.388 Section 12.0

Back